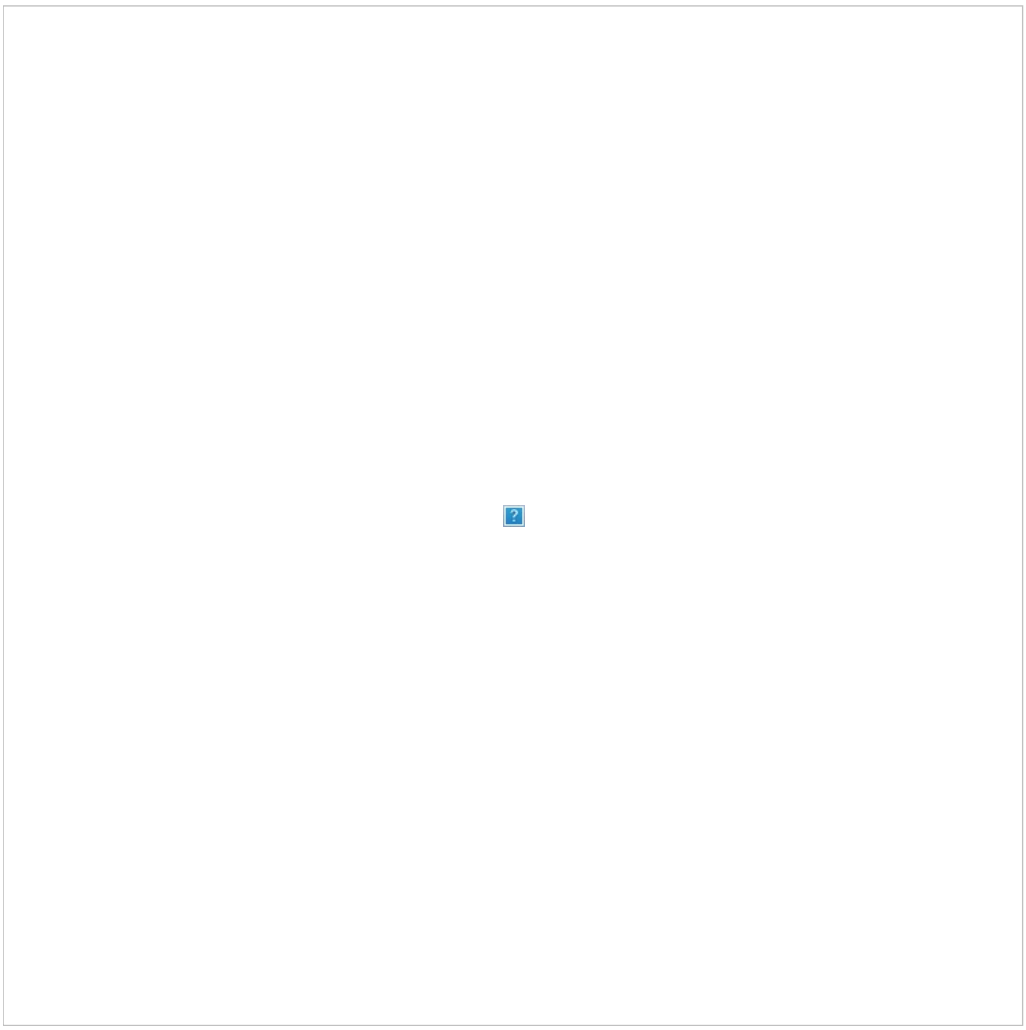
Article Number: 209 | Rating: Unrated | Last Updated: Thu, Jul 26, 2018 at 10:31 AM

Preventing certificate warnings

Posted on July 26th



In this recipe, you will prevent users from receiving a security certificate (https://cookbook.fortinet.com/glossary/certificate/) warning when your FortiGate applies full SSL inspection (https://cookbook.fortinet.com/glossary/ssl-inspection/) to incoming traffic.

When full SSL inspection is used, your FortiGate impersonates the recipient of the originating SSL (https://cookbook.fortinet.com/glossary/ssl/) session (https://cookbook.fortinet.com/glossary/session/), then decrypts and inspects the content. The FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender, and sends the content to the end user. This is the same process used in “man-in-the-middle” attacks, which is why a user’s device may show a security certificate warning.

For more information about SSL inspection, see Why you should use SSL inspection (https://cookbook.fortinet.com/why-you-should-use-ssl-inspection/).

Often, when a user receives a security certificate warning, they simply select **Continue**without understanding why the error is occurring. To avoid encouraging this habit, you can prevent the warning from appearing in the first place.

There are two methods for doing this, depending on whether you are using your FortiGate’s default certificate (https://cookbook.fortinet.com/preventing-certificate-warnings-54/#default) or using a self-signed certificate (https://cookbook.fortinet.com/preventing-certificate-warnings-54/#custom).

Find this recipe for other FortiOS versions

5.2 (https://cookbook.fortinet.com/preventing-certificate-warnings-54/#default) (https://cookbook.fortinet.com/preventing-certificate-warnings-defaultcert-56/)

Using the default certificate

All FortiGates have a default certificate that is used for full SSL inspection. This certificate is also used in the default **deep-inspection** profile. To prevent your users from seeing certificate warnings, you can install this certificate on your users' devices.

If you have the right environment, you can distribute the certificate and have it installed automatically.

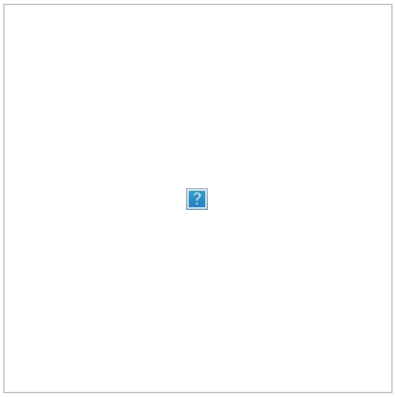
1. Generating a unique certificate

Run the following CLI (https://cookbook.fortinet.com/glossary/cli/) command to make sure that your SSL certificate is unique to your FortiGate:

```
exec vpn certificate local generate default-ssl-ca
```

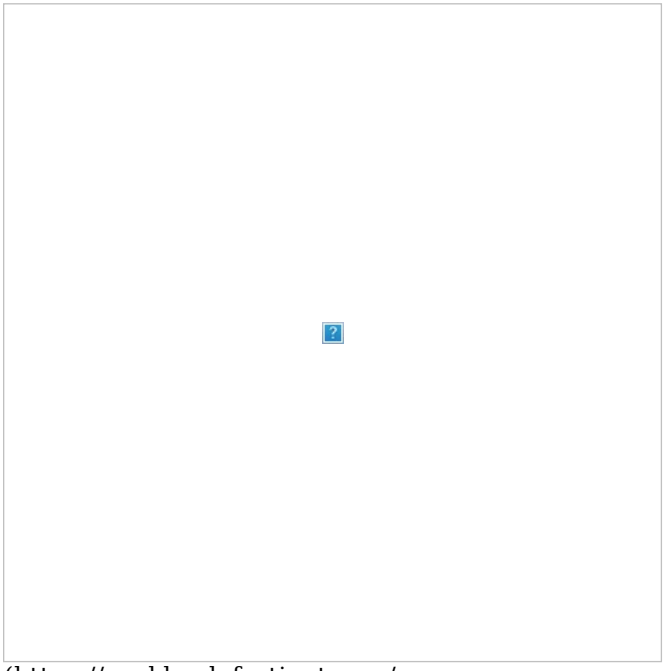
2. Downloading the certificate used for full SSL inspection

Go to **Security Profiles > SSL/SSH (https://cookbook.fortinet.com/glossary/ssh/) Inspection**. Use the dropdown menu in the top right corner to select **deep-inspection**, the profile used to apply full SSL inspection.



(https://cookbook.fortinet.com/wp-content/uploads/FortiGate/54/prevent-certificate-errors/1a-dropdown.png)

The default FortiGate certificate is listed as the **CA (https://cookbook.fortinet.com/glossary/ca/) Certificate**. Select **Download Certificate**.



(https://cookbook.fortinet.com/wp-content/uploads/FortiGate/54/prevent-certificate-errors/1b-download-cert.png)

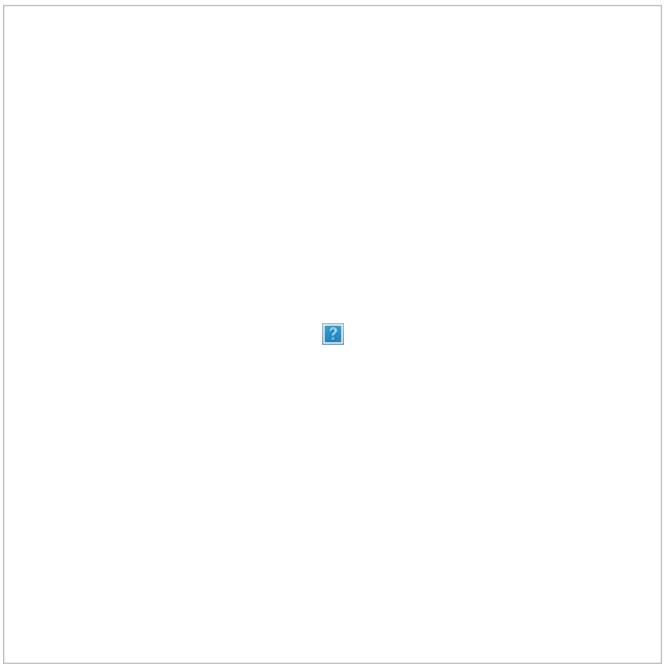
3. Installing the certificate on the user’s browser

Internet Explorer, Chrome, and Safari (on Windows or Mac OS):

The above browsers use the operating system’s certificate store for Internet browsing. If your users will be using these applications, you must install the certificate into the certificate store for your OS.

If you are using Windows 7/8/10, double-click on the certificate file and select **Open**. Select **Install Certificate** to launch the **Certificate Import Wizard**.

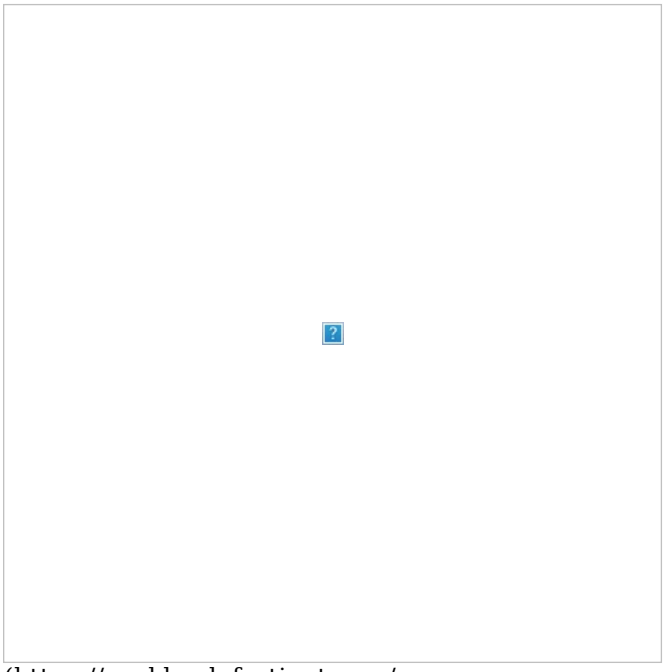
Use the wizard to install the certificate into the **Trusted Root Certificate Authorities** store. If a security warning appears, select **Yes** to install the certificate.



(https://cookbook.fortinet.com/wp-content/uploads/FortiGate/54/prevent-certificate-errors/2a-windows.png)

If you are using Mac OS X, double-click on the certificate file to launch **Keychain Access.**

Locate the certificate in the **Certificates** list and select it. Expand **Trust** and select **Always Trust**. If necessary, enter the administrative password for your computer to make this change.



(https://cookbook.fortinet.com/wp-content/uploads/FortiGate/54/prevent-certificate-errors/2b-mac-os.png)

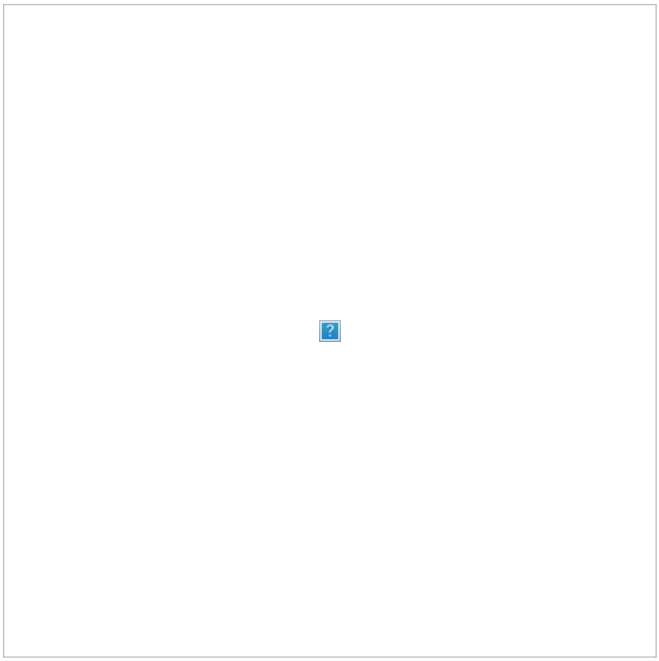
If you have the right environment, the certificate can be pushed to your users' devices. However, if Firefox is used, the certificate must be installed on each individual device, using the instructions below.

Firefox (on Windows or Mac OS)

Firefox has its own certificate store. To avoid errors in Firefox, then the certificate must be installed in this store, rather than in the OS.

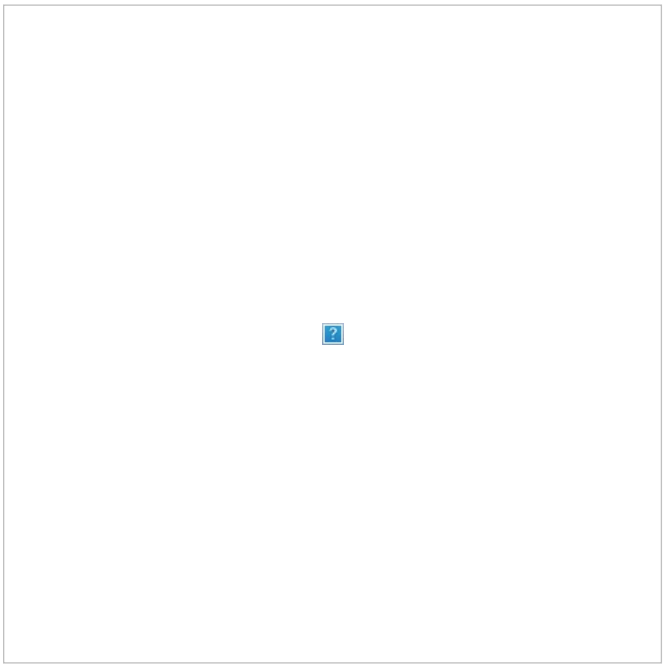
Go to **Tools > Options > Advanced** or **Firefox >Preferences > Advanced**and find the **Certificates**tab.

Select **View Certificates**, then select the **Authorities** list. **Import** the certificate and set it to be trusted for website identification.


(https://cookbook.fortinet.com/wp-content/uploads/FortiGate/54/prevent-certificate-errors/2c-firefox.png)

4. Results

Before installing the certificate, an error message would appear in the browser when a site that used HTTPS (https://cookbook.fortinet.com/glossary/https/) was accessed (the example shows an error message appearing in Firefox).


(https://cookbook.fortinet.com/wp-content/uploads/FortiGate/54/prevent-certificate-errors/3a-error.png)

After you install the certificate, you should not experience a certificate security issue when you browse to sites on which the FortiGate unit performs SSL content inspection.

If you view information about the connection, you will see that it is verified by Fortinet.

(https://cookbook.fortinet.com/wp-content/uploads/FortiGate/54/prevent-certificate-errors/3b-verified-Fortinet.png)

Posted by: Les Carr - Thu, Jul 26, 2018 at 10:31 AM. This article has been viewed 9621 times.

Online URL: https://kb.ic.uk/article/full-deep-ssl-inspection-avoid-certificate-errors-209.html (https://kb.ic.uk/article/full-deep-ssl-inspection-avoid-certificate-errors-209.html)